

図5に示した携帯電話機100の構成と異なる点は、まず、メモリカード180が装着されていること以外に、携帯電話機101は、公開暗号化キーK_{pp}を保持して、再生モード時にキーK_{pp}をデータバスBS2に出力するK_{pp}保持部1524を備える構成となっていることである。

- 5 さらに、携帯電話機101は、秘密復号キーK_pを保持するK_p保持部1520と、このK_p保持部1520から与えられるキーK_pに基づいて、データバスBS2を介してメモリカード180から与えられるキーK_{pp}で暗号化されたセッションキーK_s1を復号し抽出する復号処理部1522とをさらに備える構成となっている。しかも、暗号化処理部1504は、この復号処理部1522から
10 与えられるセッションキーK_s1により、K_s発生部1502からの自身のセッションキーK_sを暗号化してデータバスBS2に出力する。

携帯電話機101のその他の点は、図5に示した実施例1の携帯電話機100の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

- 15 図27は、実施例7のメモリカード180に対応したコンテンツサーバ11の構成を示す概略ブロック図である。図3に示したコンテンツサーバ10の構成と異なる点は、データ処理部310における暗号化処理部322は、K_s発生部314からのセッションキーK_sに基づいてではなく、携帯電話機に装着されたメモリカードからセッションキーK_sにより暗号化されて送信され、復号処理部318により復号抽出されたセッションキー、たとえば、セッションキーK_s1に基づいて、暗号化処理部320の出力をさらに暗号化して、データバスBS1を介して通信装置350に与える点である。
20

- コンテンツサーバ11のその他の点は、図3に示した実施例1のコンテンツサーバ10の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。
25

図28は、本発明の実施例7のメモリカード180の構成を説明するための概略ブロック図であり、実施例4の図18と対比される図である。

メモリカード180の構成が、メモリカード150の構成と異なる点は、まず、セッションキーK_s1発生部1432は、このカード独自のセッションキーK_s

1を発生することである。

メモ리카ード180は、さらに、カードという媒体に固有の公開暗号化キーK Pmediaを保持するK Pmedia保持部1440の出力と、データバスBS3を介して携帯電話機101から与えられる公開暗号化キーK Ppとを受けて、動作モードに応じていずれか一方を出力する切換えスイッチ1436を備える。切換えスイッチ1436は、接点PiおよびPhとを有し、接点PiはデータバスBS3と、接点PhはK Pmedia保持部1440とそれぞれ結合する。暗号化処理部1430は、切換えスイッチ1436から与えられる公開暗号化キーK Pmediaまたは公開暗号化キーK Ppのいずれかにより、Ks1発生部1432からのセッションキーKs1を暗号化して、データバスBS3に与える。

すなわち、切換えスイッチ1436は、配信モードのとき、および移動モードにおいて移動先となっているときは、未使用状態であり、再生モードの時は、接点Piの側に閉じており、移動モードにおいて移動元となっているときは、接点Phの側に閉じている。

メモ리카ード180は、さらに、接点Pe、PfおよびPgを有し、復号処理部1404から与えられるコンテンツサーバ11からのセッションキーKsと、Ks1発生部1432の出力と、データバスBS4から与えられる携帯電話機101からのセッションキーKsとを受けて、動作モードに応じていずれか1つを選択的に出力する切換えスイッチ1435を、切換えスイッチ1434の替わりに備える。接点Peには復号処理部1404からの出力が、接点PfにはKs1発生部1432の出力が、接点PgにはデータバスBS4がそれぞれ結合している。したがって、暗号化処理部1406と復号処理部1410は、この切換えスイッチ1435から与えられるキーに基づいて、それぞれ、暗号化処理および復号処理を行なう。

すなわち、切換えスイッチ1435は、配信モードの場合にコンテンツサーバ11からのセッションキーの抽出を行なうときは、接点Peの側に閉じており、配信モードの場合に配信サーバからの暗号化されたライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDについてキーKs1による復号を行なうときは、接点Pfの側に閉じている。切換えスイ

ッチ 1 4 3 5 は、再生モードにおいて復号処理を行なうときは、接点 P f の側に閉じており、再生モードにおいて暗号化処理を行なうときは、接点 P g の側に閉じている。切換えスイッチ 1 4 3 5 は、移動モードにおいて移動元となっている場合に復号処理を行うときは、接点 P f の側に閉じており、移動モードにおいて移動元となっている場合に暗号化処理を行うときは、接点 P g の側に閉じている。切換えスイッチ 1 4 3 5 は、移動モードにおいて移動先となっている場合に移動元のセッションキーを受け取るときは、接点 P e の側に閉じており、移動モードにおいて移動先となっている場合にライセンスキー K c、ライセンス ID データ License-ID およびユーザ ID データ User-ID を受け取るときは、接点 P f の側に閉じている。

メモリカード 1 8 0 は、さらに、接点 P a、P b、P c および P e を有し、K s 1 発生部 1 4 3 2 から与えられる自身のセッションキー K s 1 と、K P c a r d 保持部 1 4 0 5 の出力と、データバス B S 5 から与えられるライセンスキー K c と、暗号化処理部 1 4 1 4 から与えられ、相手方の公開暗号化キー K P c a r d (n) により暗号化されたライセンスキー K c、ライセンス ID データ License-ID およびユーザ ID データ User-ID とを受けて、動作モードに応じていずれか 1 つを選択的に出力する切換えスイッチ 1 4 0 9 を、切換えスイッチ 1 4 0 8 の替わりに備える。接点 P a には K s 1 発生部 1 4 3 2 からの出力が、接点 P b には K P c a r d 保持部 1 4 0 5 の出力が、接点 P c にはデータバス B S 5 が、接点 P d には暗号化処理部 1 4 1 4 の出力が、それぞれ結合している。したがって、暗号化処理部 1 4 0 6 は、この切換えスイッチ 1 4 0 9 から与えられるデータに対して、それぞれ、暗号化処理を行なう。

すなわち、切換えスイッチ 1 4 0 9 は、配信モードにおいて、配信先となっている場合にコンテンツサーバ 1 1 に自身の公開暗号化キー K P c a r d (1) や自身のセッションキー K s 1 を送信するときは、順次、接点 P b の側および接点 P a の側に閉じる。切換えスイッチ 1 4 0 9 は、再生モードのときは、接点 P c の側に閉じており、移動モードにおいて移動元となっているときは、接点 P d の側に閉じている。切換えスイッチ 1 4 0 9 は、移動モードにおいて移動先となっている場合にも移動元に自身の公開暗号化キー K P c a r d (1) や自身のセッ

セッションキーKs1を送信するときは、順次、接点Pbの側および接点Paの側に閉じる。

図29は、図28で説明したメモリカード180を用いた配信モードを説明するためのフローチャートである。

- 5 図28においては、ユーザ1が、メモリカード180を用いることで、コンテンツサーバ11からコンテンツデータの配信を受ける場合の動作を説明している。

まず、ユーザ1の携帯電話機101から、ユーザのタッチキー1108の操作等によって、コンテンツサーバ11に対して配信リクエストがなされる（ステップS100）。

- 10 コンテンツサーバ11においては、この配信リクエストに応じて、セッションキー発生部314が、セッションキーKsを生成する（ステップS103）。一方、メモリカード180の側では、Ks1発生部1432がセッションキーKs1を生成する（ステップS103'）。

- 15 コンテンツサーバ11では、続いて、コンテンツサーバ11内の暗号化処理部316が、公開暗号化キーKpmediaにより、セッションキーKsを暗号化処理して、データバスBS1に与える（ステップS104）。

通信装置350は、暗号化処理部316からの暗号化セッションキー[Ks]Kmediaを、通信網を通じて、携帯電話機101のメモリカード180に対して送信する（ステップS106）。

- 20 メモリカード180においては、メモリインタフェース1200を介して、データバスBS3に与えられた受信データを、復号処理部1404が、秘密復号キーKmediaにより復号処理することにより、セッションキーKsを復号し抽出する（ステップS108）。

- 25 続いて、配信モードにおいては、まず、切換えスイッチ1409が接点Pbが閉じる状態が選択されているので、暗号化処理部1406は、接点Pbを介してKpcard(1)保持部1405から与えられる公開暗号化鍵Kpcard(1)（ユーザ1のメモリカードにおける公開暗号化鍵）を受け取り、続いて、切換えスイッチ1409が接点Paが閉じる状態となって、暗号化処理部1406は、接点Paを介してKs1保持部1432から与えられるセッションキーK

s 1を受け取る。暗号化処理部1406は、切換えスイッチ1435が接点Pcが閉じる状態が選択されているので、復号処理部1404からのセッションキーKsにより、公開暗号化鍵Kp card (1) およびセッションキーKs 1を暗号化してデータベースBS3に与える。

- 5 携帯電話機101は、暗号化処理部1406により暗号化されたデータ[KP card (1)、Ks 1] Ksをコンテンツサーバ11に対して出力する(ステップS112)。

サーバ31では、通信装置350により受信され、データベースBS1に与えられたデータ[KP card (1)、Ks 1] Ksを復号処理部318が、セッションキーKsにより復号化処理して、公開暗号化キーKP card (1) およびセッションキーKs 1を復号抽出する(ステップS114)。

続いて、配信制御部312は、ライセンスキーKcを配信情報データベース304より取得し(ステップS116)。かつ、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータLicense-IDおよびユーザIDデータUser-ID等のデータを生成する(ステップS118)。

暗号化処理部320は、配信制御部312からのライセンスキーKc、ライセンスIDデータLicense-IDおよびユーザIDデータUser-ID等のデータを受取って、復号処理部318より与えられた公開暗号化キーKP card (1) により暗号化処理する(ステップS120)。

20 暗号化処理部322は、暗号化処理部320により暗号化されたデータを受取って、さらにセッションキーKs 1により暗号化して、データベースBS1に与える(ステップS122)。

通信装置350は、暗号化処理部322により暗号化されたデータ[[Kc, License-ID, User-ID] Kcard (1)] Ks 1をカード180に対して送信する。

25 カード180においては、切換えスイッチ1435が接点Pfが閉じる状態が選択される状態に切換えられているので、復号処理部1410は、Ks 1発生部1432からのセッションキーKs 1により、復号処理を行ない、データ[Kc, License-ID, User-ID] Kcard (1) を抽出し(ステップ

S126)、メモリ1412に格納する(ステップS128)。

さらに、メモリカード180においては、復号処理部1416が、メモリ1412に格納されたデータ[Kc, License-ID, User-ID] Kc
card(1)を復号し、復号されたデータLicense-ID, User-ID
5 Dをコントローラ1420が、レジスタ1500に格納する(ステップ129)。

一方、コンテンツサーバ11は、暗号化コンテンツデータ[Dc] Kcを配信
情報データベース304より取得して、通信装置350を介して、メモリカード
180に送信する(ステップS130)。

メモリカード180においては、受信した暗号化コンテンツデータ[Dc] K
10 cをそのままメモリ1412に格納する(ステップS132)。

以上のような動作により、メモリカード180は、コンテンツデータを再生可
能な状態となる。

図30は、携帯電話機101内において、実施例7のメモリカード180に保
持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽とし
15 て外部に出力するための再生モードを説明するフローチャートである。

図30を参照して、携帯電話機のタッチキー1108等からのユーザ1の指示
により、再生リクエストがメモリカード180に対して出力される(ステップS
200)。

メモリカード180では、コントローラ1420がレジスタ1500からライ
20 センスIDデータLicense-ID、ユーザIDデータUser-ID等を読
出す(ステップS205)。

コントローラ1420は、復号化されたライセンスIDデータLicense
-ID等に含まれる情報に基づいて、ライセンスIDデータLicense-I
D中のデータにより指定されるコンテンツデータ(音楽データ)の再生処理の累
25 算数が、再生可能回数の上限值を超えているかいないかを判断し(ステップS2
06)、再生可能回数を超えていないと判断した場合は、携帯電話機101のコ
ントローラ1106に対して、再生許可通知を送信する(ステップS208)。

携帯電話機101においては、まず、公開暗号化キーKppをメモリカード1
80に対して送信し、セッションキー発生回路1502がセッションキーKsを

生成する（ステップS210）。

一方、メモ리카ード180でもセッションキーKs1を生成し（ステップS210'）、公開暗号化キーKpでセッションキーKs1を暗号化して（ステップS211）、携帯電話機101に暗号化セッションキー[Ks1]Kpを送信する（ステップS212）。

携帯電話機101では、復号処理部1522が秘密復号キーKpにより、データバスBS2を介してメモ리카ード180から与えられた暗号化セッションキー[Ks1]Kpを復号し、セッションキーKs1を抽出し（ステップS213）、暗号化処理部1504が、セッションキーKs1によりセッションキーKsを暗号化して（ステップS214）、データバスBS2に暗号化セッションキー[Ks]Ks1が出力される（ステップS215）。

メモ리카ード180は、データバスBS3を介して、携帯電話機101により生成された暗号化セッションキー[Ks]Ks1を受け取り、セッションキーKs1により復号し、セッションキーKsを抽出する（ステップS216）。

さらに、メモ리카ード180は、再生処理が行われることに応じて、レジスタ1500中のライセンスIDデータLicense-IDのうち、再生処理の累積数に関するデータを更新する（ステップ217）。

続いて、メモ리카ード180は、メモリ1412から、暗号化されているデータ[Kc, License-ID, User-ID]Kcard(1)を読み出し、復号処理部1416が復号してライセンスキーKcを抽出する（ステップS218）。

続いて、抽出したセッションキーKsにより、ライセンスキーKcを暗号化し（ステップS219）、暗号化ライセンスキー[Kc]KsをデータバスBS2に与える（ステップS220）。

携帯電話機101の復号処理部1506は、セッションキーKsにより復号化処理を行なうことにより、ライセンスキーKcを取得する（ステップS222）。

続いて、メモ리카ード180は、暗号化コンテンツデータ[Dc]Kcをメモリ1412から読み出し、データバスBS2に与える（ステップS224）。

携帯電話機の音楽再生部1508は、暗号化コンテンツデータ[Dc]Kcを、

抽出されたライセンスキーKcにより復号処理し（ステップS226）、コンテンツデータを再生して混合部1510に与える（ステップS228）。

一方、ステップS206において、コントローラ1420が復号処理は不可能であると判断した場合、メモリカード180は、携帯電話機101に対して、再生不許可通知を送信する（ステップS230）。

以上のような構成とすることで、メモリカードおよび携帯電話機が独自のセッションキーを生成する場合でも、ユーザがコンテンツデータを再生できる回数を制限することが可能である。

図31は、実施例7の2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するためのフローチャートである。

図31を参照して、まず、図31においては、携帯電話機101が送信側であり、これと同様の構成を有する携帯電話機103が受信側であるものとする。また、携帯電話機103にも、メモリカード180と同様の構成を有するメモリカード182が装着されているものとする。

携帯電話機101は、まず、自身の側のメモリカード180と、受信側の携帯電話機103に挿入されたメモリカード182に対して、移動リクエストを出力する（ステップS300）。

これに応じて、携帯電話機101においては、メモリカード180内のセッションキー発生回路1432は、セッションキーKs1を生成し（ステップS312）、一方、携帯電話機103においては、メモリカード182内のセッションキー発生回路1432は、セッションキーKs2を生成する（ステップS312）。

携帯電話機101においては、メモリカード180は、公開暗号化キーKpmediaを用いて、暗号化処理部1430がセッションキーKs1を暗号化して（ステップS314）、たとえば、トランシーバモードではアンテナ1102を介して、暗号化セッションキー[Ks]Kmediaをメモリカード182に伝達する（ステップS316）。

メモリカード182においては、復号処理部1404が、秘密復号キーKmediaにより、セッションキーKs1を復号抽出し（ステップS320）、さら

に、セッションキーKs1によりメモリカード182の公開暗号化キーK P c a r d (2) およびセッションキーKs2を暗号化して(ステップS322)。メモリカード180に対して、暗号化されたデータ[K P c a r d (2)、Ks2] Ks1を送信する(ステップS324)。

- 5 メモリカード180においては、メモリカード182から送信された暗号化データを復号処理部1410がセッションキーKs1により復号化して、メモリカード182の公開暗号化キーK P c a r d (2) およびセッションキーKs2を復号抽出する(ステップS326)。このとき、切換えスイッチ1435では接点Pfが閉じており、Ks1発生回路1432からのキーKs1が復号処理部1410に与えられている。

- 10 続いて、メモリカード180においては、メモリ1412からメモリカード150の公開暗号化キーK c a r d (1) により暗号化されているライセンスキーKc、ライセンスIDデータL i c e n s e - I D およびユーザIDデータU s e r - I D が読出される(ステップS328)。

- 15 続いて、復号処理部1416が、秘密復号キーK c a r d (1) により、ライセンスキーKc、ライセンスIDデータL i c e n s e - I D、ユーザIDデータU s e r - I D とを復号処理する(ステップS330)。

- 20 コントローラ1420は、このようにして復号されたライセンスキーKc、ライセンスIDデータL i c e n s e - I D、ユーザIDデータU s e r - I D の値を、レジスタ1500内のデータ値と置換する(ステップS331)。

さらに、暗号化処理部1414は、復号処理部1410において抽出されたカード182における公開暗号化キーK P c a r d (2) により、ライセンスキーKc、ライセンスIDデータL i c e n s e - I D、ユーザIDデータU s e r - I D とを暗号化する(ステップS332)。

- 25 暗号化処理部1414により暗号化されたデータは、切換えスイッチ1409(接点Pdが閉じている)を介して、さらに、暗号化処理部1406に与えられ、暗号化処理部1406は、データ[Kc、L i c e n s e - I D、U s e r - I D] K c a r d (2) をメモリカード182のセッションキーKs2により暗号化する(ステップS334)。このとき、切換えスイッチ1435は、接点Pg

が閉じており、復号処理回路1410からのセッションキーKs2が暗号化処理部1406に与えられている。

続いて、メモリカード180は、携帯電話機101を介して、メモリカード152に対して、暗号化されたデータ[[Kc, License-ID, User-ID] Kcard(2)] Ks2を送信する(ステップS336)。

メモリカード182においては、メモリカード180から送信されたデータを復号処理部1410により、セッションキーKs2に基づいて復号化処理して、メモリ1412に格納する(ステップS339)。さらに、メモリカード182は、ライセンスキーKcard(2)に基づいて、データ[Kc, License-ID, User-ID] Kcard(2)を復号し、復号されたライセンスIDデータLicense-ID、ユーザIDデータUser-IDをレジスタ1500に格納する(ステップS341)。

一方、メモリカード180は、さらに、レジスタ1500に格納されたライセンスIDデータLicense-IDおよびユーザIDデータUser-IDを消去する(ステップS343)。

続いて、メモリカード180は、暗号化コンテンツデータ[Dc] Kcをメモリから読出し、メモリカード182に対して送信する(ステップS344)。

メモリカード182は、受信した暗号化コンテンツデータをそのままメモリ1412に格納する(ステップS346)。

以上のような処理を行なうと、ステップS342において、ライセンスキーKc、ライセンスIDデータLicense-IDおよびユーザIDデータUser-ID等がメモリカード180からは消去されているので、メモリカード180は「状態SB」となる。

一方、メモリカード182においては、暗号化コンテンツデータ以外にも、ライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-ID等のすべてのデータが移動されているので、メモリカード182は「状態SA」となっている。

以上のような構成を用いることで、たとえば、メモリカード180からメモリカード182へのデータの移動を、上述したようなセッションキー発生回路15

02を有する携帯電話機を介さず、メモ리카ードとメモ리카ードとを接続可能なインタフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

5 しかも、ライセンスIDデータLicense-ID等は、レジスタ1500に格納され、コントローラ1420はそれを参照すればよいので、動作に必要な処理量を低減できる。

さらに、セッションキーが、携帯電話機、メモ리카ードの各々で異なるため、通信のセキュリティが一層向上する。

10 ここで、移動時には、再生情報内の再生回数を制限するライセンスIDデータLicense-IDについては、メモリ1412に記録されたライセンスIDデータLicense-IDを、レジスタ1500にて再生の都度修正された再生回数を記録したライセンスIDデータLicense-IDに変更して、新たな再生情報を構成する。このようにして、メモ리카ード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決
15 められた再生回数の制限を越えることがないようにすることが可能である。

〔実施例8〕

実施例8の携帯電話機105およびメモ리카ード190は、以下に説明するように、実施例7の携帯電話機101およびメモ리카ード180の構成とは、以下の点で異なることを特徴とする。

20 すなわち、実施例8の携帯電話機105では、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこの携帯電話機105を登録する際に、この携帯電話機105に割当てられた公開暗号化鍵K_{PP}および認証データC_{rtf}とを公開復号鍵（公開認証鍵）K_{Pmaster}により暗号化された形で記録保持する手段を有している。

25 同様に、実施例8のメモ리카ード190でも、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこのメモ리카ード190を登録する際に、このメモ리카ードに割当てられた公開暗号化鍵K_{Pmedia}および認証データC_{rtf}とを公開復号鍵（公開認証鍵）K_{Pmaster}により暗号化された形で記録保持する手段を有している。

ここで、メモ리카ード190および実施例8のコンテンツサーバ12には、この公開復号鍵（公開認証鍵）K P m a s t e r を記録保持する手段を有している。この公開復号鍵（公開認証鍵）K P m a s t e r は、システム中でデータ出力を行なう全ての機器がセッションキーにやりとりに対して、相互にデータの授受を行なえる機器であることの証明と、セッションキーを相手方に送付する際に用いる暗号鍵の獲得に用いるシステム共通の鍵である。

以下、さらに、実施例8の携帯電話機105、メモ리카ード190およびコンテンツサーバ12の構成をより詳しく説明する。

図32は、実施例8における携帯電話機105の構成を説明するための概略ブロック図である。

図26に示した携帯電話機101の構成と異なる点は、K P p 保持部1524の替わりに、公開復号鍵（公開認証鍵）K P m a s t e r により暗号化された、公開暗号鍵K P p および認証データC r t f を保持するための[K P p, C r t f] K P m a s t e r 保持部1525を備える構成となっていることである。

携帯電話機105のその他の点は、図26に示した実施例7の携帯電話機101の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰返さない。

図33は、実施例8のメモ리카ード190に対応したコンテンツサーバ12の構成を示す概略ブロック図である。図27に示したコンテンツサーバ11の構成と異なる点は、データ処理部310は、公開復号鍵K P m a s t e r を保持するK P m a s t e r 保持部324と、K P m a s t e r 保持部324から出力される公開復号キーK P m a s t e r に基づいて、通信網から通信装置350を介してデータバスB S 1に与えられるデータを復号するための復号処理部326とをさらに備える構成となっている点である。暗号化処理部316は、復号処理部326での復号処理により抽出された公開暗号化キーK P m e d i a により、K s 発生部314で発生されたセッションキーK s を暗号化し、また、配信制御部312は、復号処理部326での復号処理により抽出された認証データC r t f により、配信を求めてきたメモ리카ードが正規のメモ리카ードであるかの認証を行なう。

コンテンツサーバ１２のその他の点は、図２７に示した実施例７のコンテンツサーバ１１の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図３４は、本発明の実施例８のメモリカード１９０の構成を説明するための概略ブロック図であり、実施例７の図２８と対比される図である。

実施例８のメモリカード１９０の構成が、実施例７のメモリカード１８０の構成と異なる点は、まず、メモリカード１９０は、公開暗号鍵 KP_{media} および証明データ $Crtf$ とを公開復号鍵（公開認証鍵） KP_{master} により暗号化された形で記録保持する $[KP_{media}, Crtf]$ KP_{master} 保持部１４４２を備える構成となっていることである。一方で、切換えスイッチ１４３６は省略され、 $[KP_{media}, Crtf]$ KP_{master} 保持部１４４２の出力は直接データバス BS_3 に与えられる。

さらに、メモリカード１９０は、公開復号鍵 KP_{master} を記録保持するための KP_{master} 保持部１４５０と、 KP_{master} 保持部１４５０から出力される公開復号キー KP_{master} に基づいて、データバス BS_3 上のデータを復号するための復号処理部１４５２とを備える。

復号処理部１４５２での復号処理により抽出される公開暗号化鍵 KP_{media} および認証データ $Crtf$ のうち、公開暗号化鍵 KP_{media} は、暗号化処理部１４３０に与えられ、認証データ $Crtf$ は、データバス BS_5 を介して、コントローラ１４２０に与えられる。

メモリカード１９０のその他の構成は、図２８に示したメモリカード１８０の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

図３５は、図３４に示したメモリカード１９０内の記録空間の構成を示す概略図である。メモリカードが独自に管理して、ユーザが自由にその内容を書き換えることも読み出すこともできず、かつ、不当な開封処理に対しては、内部のデータが破壊される TRM モジュールにより構成されるセキュリティー領域１４９０、ユーザからデータの存在は確認できるものの、そのデータがメモリカード固有の暗号化、ここでは公開暗号化鍵 $KP_{card}(1)$ による暗号化が施され記録され、データの書き換えが自由に行なえない準セキュリティー領域１４９１と、コ

ユーザがその内容を自由に読み出し、書き換えが行なえる非セキュリティ領域1492とを備える。

セキュリティ領域1490には、メモ리카ード190の出荷時から保持する鍵の保持部、すなわち、Kmedia保持部1402、KPCard(1)保持部1405、Kcard(1)保持部1415、[KPmedia、Crtf]KPMaster保持部1442、KPMaster保持部1450と、平文のライセンス情報が格納されるレジスタ1500が設けられる。

準セキュリティ領域1491には、メモ리카ード1900固有の暗号化をされたデータである[Kc、Licence-ID、User-ID]Kcard(1)が格納され、メモリ1412内に設けられる。

非セキュリティ領域1493には、暗号化コンテンツデータ[Dc]Kcが格納され、メモリ1412内に設けられる。したがって、暗号化コンテンツデータ[Dc]Kcは自由に複製することが可能となるが、再生に必要なデータが複製できない構成になっている。準セキュリティ領域1491に格納されたライセンス情報を他のメモ리카ードに複製しても、メモ리카ード1900の固有の公開暗号鍵KPCard(1)にてかけられた暗号化は、対の秘密復号鍵Kcard(1)を持たない他のメモ리카ードでは複製できないからである。

また、鍵を保持する全ての鍵保持部をセキュリティ領域に設けるよう説明したが、秘密復号鍵を保持するKmedia保持部1402およびKcard(1)保持部1415のみセキュリティ領域に配置さえすれば良く、他の鍵保持部に保持された鍵は外部より参照できるROM(Read Only Memory)に配置されていてよい。

図36は、図35で説明したメモ리카ード190を用いた配信モードを説明するためのフローチャートである。

図36においては、ユーザ1が、メモ리카ード190を用いることで、コンテンツサーバ12からコンテンツデータの配信を受ける場合の動作を説明している。

まず、ユーザ1の携帯電話機105から、ユーザのタッチキー1108の操作等によって、メモ리카ード190に対して配信リクエストがなされる(ステップ5400)。

メモ리카ード190からは、[KPmedia、Crtf]KPmaster保持部1442から、携帯電話機105を経由して、コンテンツサーバ12に対して、暗号化データ[KPmedia、Crtf]KPmasterが送信される（ステップS402）。

5 コンテンツサーバ12においては、暗号化データ[KPmedia、Crtf]KPmasterを受信すると、KPmaster保持部324が保持する公開復号キーKPmasterに基づいて、復号処理部326が復号処理することにより、公開暗号化キーKPmediaおよび認証データCrtfを取得する（ステップS404）。

10 さらに、コンテンツサーバ12においては、認証データCrtfによりメモ리카ード190の認証を行ない（ステップS406）、メモ리카ード190が正規のメモ리카ードであることが証明されれば、処理はS412に移行する。一方、コンテンツサーバ12は、メモ리카ード190が正規のメモ리카ードであることが証明されない場合は、配信不許可通知を送信し（ステップS408）、携帯電話機105が配信不許可通知を受信する（ステップS410）。

15 メモ리카ード190が正規のメモ리카ードであることが証明された場合、コンテンツサーバ12では、セッションキー発生部314が、セッションキーKsを生成する（ステップS412）。

20 コンテンツサーバ12では、続いて、コンテンツサーバ12内の暗号化処理部316が、公開暗号化キーKPmediaにより、セッションキーKsを暗号化処理して、データベースBS1に与える（ステップS414）。

 通信装置350は、暗号化処理部316からの暗号化セッションキー[Ks]Kmediaを、通信網を通じて、携帯電話機105のメモ리카ード190に対して送信する（ステップS416）。

25 メモ리카ード190においては、メモリインタフェース1200を介して、データベースBS3に与えられた受信データを、復号処理部1404が、秘密復号キーKmediaにより復号処理することにより、セッションキーKsを復号し抽出する（ステップS418）。さらに、メモ리카ード190では、Ks1発生部1432がセッションキーKs1を生成する（ステップS420）。

続いて、配信モードにおいては、まず、切換えスイッチ1409が接点Pbが閉じる状態が選択されているので、暗号化処理部1406は、接点Pbを介してK P c a r d (1) 保持部1405から与えられる公開暗号化鍵K P c a r d (1)を受け取り、続いて、切換えスイッチ1409が接点Paが閉じる状態となつて、暗号化処理部1406は、接点Paを介してK s 1発生部1432から与えられるセッションキーK s 1を受け取る。暗号化処理部1406は、切換えスイッチ1435が接点Peが閉じる状態が選択されているので、復号処理部1404からのセッションキーK sにより、公開暗号化鍵K P c a r d (1)およびセッションキーK s 1を暗号化してデータバスBS3に与える(ステップS422)。

携帯電話機105を介して、暗号化処理部1406により暗号化されたデータ[K P c a r d (1)、K s 1] K sがコンテンツサーバ12に対して送信される(ステップS424)。

コンテンツサーバ12では、通信装置350により受信され、データバスBS1に与えられたデータ[K P c a r d (1)、K s 1] K sを復号処理部318が、セッションキーK sにより復号化処理して、公開暗号化キーK P c a r d (1)およびセッションキーK s 1を復号抽出する(ステップS426)。

続いて、配信制御部312は、ライセンスキーK cを配信情報データベース304より取得し(ステップS428)、かつ、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータL i c e n s e - I DおよびユーザIDデータU s e r - I D等のデータを生成する(ステップS430)。

暗号化処理部320は、配信制御部312からのライセンスキーK c、ライセンスIDデータL i c e n s e - I DおよびユーザIDデータU s e r - I D等のデータを受取って、復号処理部318より与えられた公開暗号化キーK P c a r d (1)により暗号化処理する(ステップS432)。

暗号化処理部322は、暗号化処理部320により暗号化されたデータを受取って、さらにセッションキーK s 1により暗号化して、データバスBS1に与える(ステップS434)。

通信装置350は、暗号化処理部322により暗号化されたデータ[[K c,

License-ID, User-ID] Kcard (1)] Ks1をメモリカード190に対して送信する(ステップS436)。

メモリカード190においては、切換えスイッチ1435が接点Pfが閉じる状態が選択される状態に切換えられているので、復号処理部1410は、Ks1
5 発生部1432からのセッションキーKs1により、復号処理を行ない、データ
[Kc, License-ID, User-ID] Kcard (1)を抽出し
(ステップS438)、メモリ1412に格納する(ステップS440)。

さらに、メモリカード190においては、復号処理部1416が、メモリ14
12に格納されたデータ[Kc, License-ID, User-ID] Kc
10 ard (1)を復号し、復号されたデータLicense-ID, User-ID
をコントローラ1420が、レジスタ1500に格納する(ステップS442)。

一方、コンテンツサーバ12は、暗号化コンテンツデータ[Dc] Kcを配信
情報データベース304より取得して、通信装置350を介して、メモリカード
180に送信する(ステップS444)。

メモリカード190においては、受信した暗号化コンテンツデータ[Dc] K
cをそのままメモリ1412に格納する(ステップS446)。

以上のような動作により、メモリカード190は、コンテンツデータを再生可
能な状態となる。

図37は、携帯電話機105内において、実施例8のメモリカード190に保
持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽とし
て外部に出力するための再生モードを説明するフローチャートである。

図37を参照して、携帯電話機のキーボード1108等からのユーザ1の指示
により、再生リクエストが携帯電話機105に与えられると(ステップS50
0)、携帯電話機105からメモリカード190に対して暗号化データ[KPp、
25. Crtf] KPmasterが送信される(ステップS502)。

メモリカード190では、復号処理部1452での公開復号キーKPmaster
による復号処理により、公開暗号化鍵KPpおよび認証データCrtfが取
得される(ステップS504)。コントローラ1420は、認証データCrtf
により携帯電話機105が正規の機器であることを認証し(ステップS506)、

正規の機器であると証明されると、処理をステップ5508に移行し、正規の機器であると証明されないと再生不許可の通知を携帯電話機105に対して送信する（ステップ5544）。

携帯電話機105が正規の機器であると証明された場合（ステップ5506）、セッションキー発生部1432がセッションキーKs1を生成する（ステップ5508）。暗号化処理部1430は、復号処理部1452からの公開暗号化キーKpに基づいて、セッションキーKs1を暗号化し（ステップ5510）、暗号化セッションキー[Ks1]Kpがメモ리카ード190から携帯電話機105に対して送信される（ステップ5512）。

携帯電話機105では、復号処理部1522での復号処理により、セッションキーKs1が復号され抽出される（ステップ5514）。続いて、セッションキー発生部1502においてセッションキーKsが生成され（ステップ5516）、暗号化処理部1504がセッションキーKs1によりキーKsを暗号化して（ステップ5518）、携帯電話機105からメモ리카ード190に対して、暗号化セッションキー[Ks]Ks1が送信される（ステップ5520）。

メモ리카ード190では、復号処理部1410がセッションキーKs1により、暗号化セッションキー[Ks]Ks1を復号処理してセッションキーKsを抽出する（ステップ5522）。さらに、メモ리카ード190では、コントローラ1420がレジスタ1500からライセンスIDデータLicense-ID、ユーザIDデータUser-ID等を読出す（ステップ5524）。

コントローラ1420は、復号化されたライセンスIDデータLicense-ID等に含まれる情報に基づいて、ライセンスIDデータLicense-ID中のデータにより指定されるコンテンツデータ（音楽データ）の再生処理の累積数が、再生可能回数の上限値を超えているかいないかを判断し（ステップ5526）、再生可能回数を超えていないと判断した場合は、メモ리카ード190は、再生処理が行われることに応じて、レジスタ1500中のライセンスIDデータLicense-IDのうち、再生処理の累積数に関するデータを更新する（ステップ5528）。

続いて、メモ리카ード190は、メモリ1412から、暗号化されているデー

タ [Kc, License-ID, User-ID] Kcard (1) を読み出し、復号処理部 1416 が復号してライセンスキー Kc を抽出する (ステップ S530)。

- 5 続いて、ステップ S522 において抽出したセッションキー Ks により、ライセンスキー Kc を暗号化し (ステップ S532)。暗号化ライセンスキー [Kc] Ks をデータバス BS2 に与える (ステップ S534)。

携帯電話機 105 の復号処理部 1506 は、セッションキー Ks により復号化処理を行なうことにより、ライセンスキー Kc を取得する (ステップ S536)。

- 10 続いて、メモリカード 190 は、暗号化コンテンツデータ [Dc] Kc をメモリ 1412 から読み出し、データバス BS2 に与える (ステップ S538)。

携帯電話機の音楽再生部 1508 は、暗号化コンテンツデータ [Dc] Kc を、抽出されたライセンスキー Kc により復号処理し (ステップ S540)、コンテンツデータを再生して混合部 1510 に与える (ステップ S542)。

- 15 一方、ステップ S526 において、コントローラ 1420 が復号処理は不可能であると判断した場合、メモリカード 190 は、携帯電話機 105 に対して、再生不許可通知を送信する (ステップ S544)。

以上のような構成とすることで、メモリカードおよび携帯電話機が独自のセッションキーを生成する場合でも、ユーザがコンテンツデータを再生できる回数を制限することが可能である。

- 20 図 38 は、実施例 8 の 2 つのメモリカード間において、コンテンツデータおよびキーデータ等の移動を行なう処理を説明するためのフローチャートである。

- 図 38 を参照して、まず、図 38 においては、携帯電話機 105 が送信側であり、これと同様の構成を有する携帯電話機 107 が受信側であるものとする。また、携帯電話機 107 にも、メモリカード 190 と同様の構成を有するメモリカード 192 が装着されているものとする。

携帯電話機 105 は、まず、受信側の携帯電話機 107 に挿入されたメモリカード 192 に対して、移動リクエストを出力する (ステップ S600)。

これに応じて、携帯電話機 107 に装着されたメモリカード 192 からは、メモリカード 190 に対して、暗号化データ [Kpmedia, Crtf] Kpma

sterが送信される（ステップS602）。

メモ리카ード190においては、暗号化データ[KPmedia、Crtf]K
Pmasterを受信すると、Kmaster保持部1450が保持する公開
復号キーKmasterに基づいて、復号処理部1452が復号処理すること
5 により、公開暗号化キーKPmediaおよび認証データCrtfを取得する
（ステップS604）。

さらに、メモ리카ード190においては、認証データCrtfによりメモ리카
ード192の認証を行ない（ステップS606）、メモ리카ード192が正規の
メモ리카ードであることが証明されれば、処理はS612に移行する。一方、メ
10モ리카ード190は、メモ리카ード192が正規のメモ리카ードであることが証
明されない場合は、移動不許可通知を送信し（ステップS608）、携帯電話機
107が移動不許可通知を受信する（ステップS610）。

メモ리카ード192が正規のメモ리카ードであることが証明された場合、メモ
リカード190では、セッションキー発生部1432が、セッションキーKs1
15 を生成する（ステップS612）。

メモ리카ード190では、続いて、暗号化処理部1430が、公開暗号化キー
KPmediaにより、セッションキーKs1を暗号化処理して、データバスB
S3に与える（ステップS614）。

メモ리카ード190からは、暗号化処理部1430からの暗号化セッションキ
ー[Ks]Kmediaを、携帯電話機105を通じて、携帯電話機107のメ
20モ리카ード192に対して送信する（ステップS616）。

メモ리카ード192においては、メモリインタフェース1200を介して、デ
ータバスBS3に与えられた受信データを、復号処理部1404が、秘密復号キ
ーKmediaにより復号処理することにより、セッションキーKsを復号し抽
25 出する（ステップS618）。さらに、メモ리카ード192では、Ks1発生器
1432と同様の構成を有するKs2発生部1432'がセッションキーKs2
を生成する（ステップS620）。

続いて、メモ리카ード192では、まず、切換えスイッチ1409が接点Pb
が閉じる状態が選択されているので、暗号化処理部1406は、接点Pbを介し

てK P c a r d (1) 保持部1405から与えられる公開暗号化鍵K P c a r d (1) を受け取り、続いて、切換えスイッチ1409が接点P a が閉じる状態となつて、暗号化处理部1406は、接点P a を介してK s 2 発生部1432 から与えられるセッションキーK s 2 を受け取る。暗号化处理部1406は、切
5 換えスイッチ1435が接点P e が閉じる状態が選択されているので、復号処理部1404からのセッションキーK s 1 により、公開暗号化鍵K P c a r d (1) およびセッションキーK s 2 を暗号化してデータバスB S 3 に与える（ステップS 6 2 2 ）。

携帯電話機107を介して、暗号化处理部1406により暗号化されたデータ
10 [K P c a r d (1) , K s 2] K s 1 がメモ리카ード190に対して送信される（ステップS 6 2 4 ）。

メモ리카ード190においては、メモ리카ード192から送信された暗号化データを復号処理部1410がセッションキーK s 1 により復号化して、メモ리카ード192の公開暗号化キーK P c a r d (2) およびセッションキーK s 2 を
15 復号抽出する（ステップS 6 2 6 ）。このとき、切換えスイッチ1435では接点P f が閉じており、K s 1 発生回路1432からのキーK s 1 が復号処理部1410に与えられている。

続いて、メモ리카ード190においては、メモリ1412から、メモ리카ード190の公開暗号化キーK c a r d (1) により暗号化されているライセンスキーK c、ライセンスIDデータL i c e n s e e - I D およびユーザIDデータU s e r - I D が読出される（ステップS 6 2 8 ）。

続いて、メモ리카ード190では、復号処理部1416が、秘密復号キーK c a r d (1) により、ライセンスキーK c、ライセンスIDデータL i c e n s e e - I D、ユーザIDデータU s e r - I D とを復号処理する（ステップS 6 3
25 0 ）。

メモ리카ード190のコントローラ1420は、このようにして復号されたライセンスキーK c、ライセンスIDデータL i c e n s e e - I D、ユーザIDデータU s e r - I D の値を、レジスタ1500内のデータ値と置換する（ステップS 6 3 2 ）。

さらに、メモ리카ード190の暗号化処理部1414は、復号処理部1410において抽出されたメモ리카ード192における公開暗号化キーK_{Pcard}(2)により、ライセンスキーK_c、ライセンスIDデータLicense-ID、ユーザIDデータUser-IDとを暗号化する(ステップS634)。

- 5 メモ리카ード190の暗号化処理部1414により暗号化されたデータは、切換えスイッチ1409(接点P_dが閉じている)を介して、さらに、暗号化処理部1406に与えられ、暗号化処理部1406は、データ[K_c, License-ID, User-ID] K_{card}(2)をメモ리카ード192のセッションキーK_{s2}により暗号化する(ステップS636)。このとき、切換えスイッチ1435は、接点P_gが閉じており、復号処理回路1410からのセッションキーK_{s2}が暗号化処理部1406に与えられている。

続いて、メモ리카ード190は、携帯電話機105を介して、メモ리카ード192に対して、暗号化されたデータ[[K_c, License-ID, User-ID] K_{card}(2)] K_{s2}を送信する(ステップS638)。

- 15 メモ리카ード192においては、メモ리카ード190から送信されたデータを復号処理部1410により、セッションキーK_{s2}に基づいて復号化処理して、メモリ1412に格納する(ステップS640)。さらに、メモ리카ード192は、ライセンスキーK_{card}(2)に基づいて、データ[K_c, License-ID, User-ID] K_{card}(2)を復号し、復号されたライセンスIDデータLicense-ID、ユーザIDデータUser-IDをレジスタ1500に格納する(ステップS642)。

一方、メモ리카ード190は、さらに、レジスタ1500に格納されたライセンスIDデータLicense-IDおよびユーザIDデータUser-IDを消去する(ステップS644)。

- 25 続いて、メモ리카ード190は、暗号化コンテンツデータ[D_c] K_cをメモリ1412から読出し、メモ리카ード192に対して送信する(ステップS646)。

メモ리카ード192は、受信した暗号化コンテンツデータをそのままメモリ1412に格納する(ステップS648)。

以上のような処理を行なうと、ステップS644において、ライセンスキーKc、ライセンスIDデータLicense-IDおよびユーザIDデータUser-ID等がメモリカード190からは消去されているので、メモリカード190は「状態SB」となる。

- 5 一方、メモリカード192においては、暗号化コンテンツデータ以外にも、ライセンスキーKc、ライセンスIDデータLicense-ID、ユーザIDデータUser-ID等のすべてのデータが移動されているので、メモリカード192は「状態SA」となっている。

- 10 ここで、実施例7と同様に、ライセンスIDデータLicense-ID等は、レジスタ1500に格納され、コントローラ1420はそれを参照すればよいため、動作に必要な処理量を低減できる。

さらに、セッションキーが、携帯電話機、メモリカードの各々で異なるため、通信のセキュリティーが一層向上する。

- 15 ここで、移動時には、再生情報内の再生回数を制限するライセンスIDデータLicense-IDについては、メモリ1412に記録されたライセンスIDデータLicense-IDを、レジスタ1500にて再生の都度修正された再生回数を記録したライセンスIDデータLicense-IDに変更して、新たな再生情報を構成する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決
20 められた再生回数の制限を越えることがないようにすることが可能である。

〔実施例9〕

図39は、実施例9のメモリカード200の構成を示す概略ブロック図である。

実施例9のメモリカード200は、以下に説明するように、実施例8のメモリカード190の構成とは、以下の点で異なることを特徴とする。

- 25 すなわち、実施例9のメモリカード200では、実施例8のメモリカード190の構成において、Kmedia保持部1402、Kpcard(1)保持部1405、Kcard(1)保持部1415、[Kpmedia、Crtf] KPmaster保持部1442、KPmaster保持部1450およびレジスタ1500が、メモリ1412の所定の領域内に設けられる構成となっている。こ

れに応じて、切換えスイッチ1409の接点PbおよびPcが省略され、データバスBS4とメモリ1412とは直接データのやり取りを行なわず、メモリ1412は、データバスBS3との間でのみデータを授受するものとする。データバスBS4は、データバスBS3を介してメモリ1412とデータの授受を行なう。

5 図40は、図39に示したメモ리카ード200内の記録空間の構成を示す概略図である。メモ리카ードが独自に管理して、ユーザが自由にその内容を書きかえることも読み出すこともできず、かつ、不当な開封処理に対しては、内部のデータが破壊されるTRMモジュールにより構成されるセキュリティ領域1490と、ユーザがその内容を自由に読み出し、書き換えが行なえる非セキュリティ領域1492とを備える。

10 セキュリティ領域1490には、メモ리카ード200の出荷時から保持する鍵の保持部、すなわち、Kmedia保持部1402、KPeard(1)保持部1405、Kcard(1)保持部1415、[KPmedia、Crtf]KPmaster保持部1442、KPmaster保持部1450と、平文のライセンス情報が格納されるレジスタ1500が設けられる。実施例8における図35と異なるのは準セキュリティ領域が設けられていない点であり、このため準セキュリティ領域1491の格納されていた[Kc、Licence-ID、User-ID]Kcard(1)をKcard(1)で復号した平文のライセンスキーKc、ライセンスID Licence-ID、ユーザID User-IDの内、実施例8においてレジスタ1500に格納されていなかったコンテンツキーKcもセキュリティ領域1490に平文で格納される。このため、実施例8に比べてセキュリティ領域1490は、より広い記録空間が必要となる。

20 非セキュリティ領域1493には、暗号化コンテンツデータ[Dc]Kcが格納され、メモリ1412がこれにあたる。したがって、暗号化コンテンツデータ[Dc]Kcは自由に複製することが可能となるが、再生に必要なデータが複製できない構成になっている。

25 また、鍵を保持する全ての鍵保持部をセキュリティ領域に設けるよう説明したが、秘密復号鍵を保持するKmedia保持部1402およびKcard(1)保持部1415のみセキュリティ領域に配置さえすれば良く、他の鍵保

持部に保持された鍵は外部より参照できるROM (Read Only Memory) に配置されていても良い。

図41は、図39で説明したメモリカード200を用いた配信モードを説明するためのフローチャートであり、実施例8の図36と対比される図である。

- 5 図41においては、ユーザ1が、メモリカード200を用いることで、コンテンツサーバ12からコンテンツデータの配信を受ける場合の動作を説明している。

まず、ユーザ1の携帯電話機105から、ユーザのタッチキー1108の操作等によって、メモリカード200に対して配信リクエストがなされる(ステップS400)。

- 10 メモリカード200からは、メモリ1412中の[KPmedia、Crtf] KPmaster保持部1442から、携帯電話機105を経由して、コンテンツサーバ12に対して、暗号化データ[KPmedia、Crtf]KPmasterが送信される(ステップS402)。

- コンテンツサーバ12においては、暗号化データ[KPmedia、Crtf] KPmasterを受信すると、KPmaster保持部324が保持する公開復号キーKPmasterに基づいて、復号処理部326が復号処理することにより、公開復号キーKPmediaおよび認証データCrtfを取得する(ステップS404)。

- さらに、コンテンツサーバ12においては、認証データCrtfによりメモリカード200の認証を行ない(ステップS406)、メモリカード200が正規のメモリカードであることが証明されれば、処理はS412に移行する。

- 一方、コンテンツサーバ12は、メモリカード200が正規のメモリカードであることが証明されない場合は、配信不許可通知を送信し(ステップS408)、携帯電話機105が配信不許可通知を受信する(ステップS410)。

- 25 メモリカード200が正規のメモリカードであることが証明された場合、コンテンツサーバ12では、セッションキー発生部314が、セッションキーKsを生成する(ステップS412)。

コンテンツサーバ12では、続いて、コンテンツサーバ12内の暗号化処理部316が、公開暗号化キーKPmediaにより、セッションキーKsを暗号化

処理して、データベースBS1に与える（ステップS414）。

通信装置350は、暗号化処理部316からの暗号化セッションキー[Ks]
Kmediaを、通信網を通じて、携帯電話機105のメモリカード200に対して送信する（ステップS416）。

- 5 メモリカード200においては、メモリインタフェース1200を介して、データベースBS3に与えられた受信データを、復号処理部1404が、データベースBS3を介してメモリ1412から与えられる秘密復号キーKmediaにより復号処理することにより、セッションキーKsを復号し抽出する（ステップS418）。さらに、メモリカード200では、Ks1発生部1432がセッション
10 キーKs1を生成する（ステップS420）。

- 続いて、配信モードにおいては、まず、暗号化処理部1406は、データベースBS3を介してメモリ1412中のKPCard(1)保持部1405から与えられる公開暗号化鍵KPCard(1)を受け取り、続いて、切換えスイッチ1409が接点Paが閉じる状態となっているので、暗号化処理部1406は、接
15 点Paを介してKs1発生部1432から与えられるセッションキーKs1を受け取る。暗号化処理部1406は、切換えスイッチ1435が接点Peが閉じる状態が選択されているので、復号処理部1404からのセッションキーKsにより、公開暗号化鍵KPCard(1)およびセッションキーKs1を暗号化してデータベースBS3に与える（ステップS422）。

- 20 携帯電話機105を介して、暗号化処理部1406により暗号化されたデータ[KPCard(1)、Ks1]Ksがコンテンツサーバ12に対して送信される（ステップS424）。

- コンテンツサーバ12では、通信装置350により受信され、データベースBS1に与えられたデータ[KPCard(1)、Ks1]Ksを復号処理部318
25 が、セッションキーKsにより復号化処理して、公開暗号化キーKPCard(1)およびセッションキーKs1を復号抽出する（ステップS426）。

続いて、配信制御部312は、ライセンスキーKcを配信情報データベース304より取得し（ステップS428）、かつ、配信情報データベース304等に保持されているデータを元に、ライセンスIDデータLicense-IDおよび

びユーザIDデータ User-ID等のデータを生成する（ステップS430）。

暗号化処理部320は、配信制御部312からのライセンスキーKc、ライセンスIDデータ License-IDおよびユーザIDデータ User-ID等のデータを受取って、復号処理部318より与えられた公開暗号化キーKpcard(1)により暗号化処理する（ステップS432）。

暗号化処理部322は、暗号化処理部320により暗号化されたデータを受取って、さらにセッションキーKs1により暗号化して、データベース1に与える（ステップS434）。

通信装置350は、暗号化処理部322により暗号化されたデータ〔〔Kc, License-ID, User-ID〕Kcard(1)〕Ks1をメモリカード200に対して送信する（ステップS436）。

メモリカード200においては、切換えスイッチ1435が接点P1が閉じる状態が選択される状態に切換えられているので、復号処理部1410は、Ks1発生部1432からのセッションキーKs1により、復号処理を行ない、データ〔Kc, License-ID, User-ID〕Kcard(1)を抽出する（ステップS438）。

さらに、メモリカード200においては、復号処理部1416が、メモリ1412中のKcard(1)保持部1415からの出力に基づいて、復号処理部1410からのデータ〔Kc, License-ID, User-ID〕Kcard(1)を復号し、復号されたライセンスIDデータ License-ID、ユーザIDデータ User-ID、ライセンスキーKcをメモリ1412中のレジスタ1500に格納する（ステップ443）。

一方、コンテンツサーバ12は、暗号化コンテンツデータ〔Dc〕Kcを配信情報データベース304より取得して、通信装置350を介して、メモリカード180に送信する（ステップS444）。

メモリカード200においては、受信した暗号化コンテンツデータ〔Dc〕Kcをそのままメモリ1412に格納する（ステップS446）。

以上のような動作により、メモリカード200は、コンテンツデータを再生可能な状態となる。

図42は、携帯電話機105内において、実施例9のメモ리카ード200に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートであり、実施例8の図37と対比される図である。

- 5 図41を参照して、携帯電話機のタッチキー1108等からのユーザ1の指示により、再生リクエストが携帯電話機105に与えられると（ステップS500）、携帯電話機105からメモ리카ード200に対して暗号化データ[KPp、Cr t f]KPmaster が送信される（ステップS502）。

- 10 メモ리카ード200では、復号処理部1452での公開復号キーKPmaster による復号処理により、公開暗号化鍵KPpおよび認証データCr t fが取得される（ステップS504）。コントローラ1420は、認証データCr t fにより携帯電話機105が正規の機器であるかを認証し（ステップS505）、正規の機器であると証明されると、処理をステップS508に移行し、正規の機器であると証明されないと再生不許可の通知を携帯電話機105に対して送信する（ステップS544）。

- 15 携帯電話機105が正規の機器であると証明された場合（ステップS506）、セッションキー発生部1432がセッションキーKs1を生成する（ステップS508）。暗号化処理部1430は、復号処理部1452からの公開暗号化キーKPpに基づいて、セッションキーKs1を暗号化し（ステップS510）、暗号化セッションキー[Ks1]Kpがメモ리카ード200から携帯電話機105に対して送信される（ステップS512）。

- 20 携帯電話機105では、復号処理部1522での復号処理により、セッションキーKs1が復号され抽出される（ステップS514）。続いて、セッションキー発生部1502においてセッションキーKsが生成され（ステップS516）、暗号化処理部1504がセッションキーKs1によりセッションキーKsを暗号化して（ステップS518）、携帯電話機105からメモ리카ード200に対して、暗号化セッションキー[Ks]Ks1が送信される（ステップS520）。

メモ리카ード200では、復号処理部1410がセッションキーKs1により、暗号化セッションキー[Ks]Ks1を復号処理してセッションキーKsを抽出

する（ステップS522）。さらに、メモ리카ード200では、コントローラ1420がメモリ1412中のレジスタ1500からライセンスIDデータLicense-ID、ユーザIDデータUser-ID等を読出す（ステップS524）。

- 5 コントローラ1420は、ライセンスIDデータLicense-ID等に含まれる情報に基づいて、ライセンスIDデータLicense-ID中のデータにより指定されるコンテンツデータ（音楽データ）の再生処理の累算数が、再生可能回数の上限値を超えているかいないかを判断し（ステップS526）、再生可能回数を超えていないと判断した場合は、メモ리카ード200は、再生処理が行われることに応じて、メモリ1412中のレジスタ1500中のライセンスIDデータLicense-IDのうち、再生処理の累算数に関するデータを更新する（ステップ528）。
- 10

- 続いて、メモ리카ード200は、メモリ1412から、ライセンスキーKcを読み出し、ステップS522において抽出したセッションキーKsにより、ライセンスキーKcを暗号化し（ステップS532）、暗号化ライセンスキー[Kc]KsをデータベースBS2に与える（ステップS534）。
- 15

携帯電話機105の復号処理部1506は、セッションキーKsにより復号化処理を行なうことにより、ライセンスキーKcを取得する（ステップS536）。

- 20 続いて、メモ리카ード200は、暗号化コンテンツキー[Dc]Kcをメモリ1412から読出し、データベースBS2に与える（ステップS538）。

携帯電話機の音楽再生部1508は、暗号化コンテンツキー[Dc]Kcを、抽出されたライセンスキーKcにより復号処理し（ステップS540）、コンテンツデータを再生して混合部1510に与える（ステップS542）。

- 一方、ステップS526において、コントローラ1420が復号処理は不可能であると判断した場合、メモ리카ード200は、携帯電話機105に対して、再生不許可通知を送信する（ステップS544）。
- 25

以上のような構成とすることで、メモ리카ードおよび携帯電話機が独自のセッションキーを生成する場合でも、ユーザがコンテンツデータを再生できる回数を制限することが可能である。

図43は、実施例9の2つのメモ리카ード間において、コンテンツデータおよびキーデータ等の移動を行なうモードを説明するためのフローチャートであり、実施例8の図38と対比される図である。

図43を参照して、まず、図43においては、携帯電話機105が送信側であり、これと同様の構成を有する携帯電話機107が受信側であるものとする。また、携帯電話機107にも、メモ리카ード200と同様の構成を有するメモ리카ード202が装着されているものとする。

携帯電話機105は、まず、受信側の携帯電話機107に挿入されたメモ리카ード202に対して、移動リクエストを出力する(ステップS600)。

これに応じて、携帯電話機107に装着されたメモ리카ード202からは、メモ리카ード200に対して、暗号化データ[KPmedia, Crtf]KPmasterが送信される(ステップS602)。

メモ리카ード200においては、暗号化データ[KPmedia, Crtf]KPmasterを受信すると、KPmaster保持部1450が保持する公開復号キーKPmasterに基づいて、復号処理部1452が復号処理することにより、公開暗号化キーKPmediaおよび認証データCrtfを取得する(ステップS604)。

さらに、メモ리카ード200においては、認証データCrtfによりメモ리카ード202の認証を行ない(ステップS606)、メモ리카ード202が正規のメモ리카ードであることが証明されれば、処理はS612に移行する。一方、メモ리카ード200は、メモ리카ード202が正規のメモ리카ードであることが証明されない場合は、移動不許可通知を送信し(ステップS608)、携帯電話機107が移動不許可通知を受信する(ステップS610)。

メモ리카ード202が正規のメモ리카ードであることが証明された場合、メモ리카ード200では、セッションキー発生部1432が、セッションキーKs1を生成する(ステップS612)。

メモ리카ード200では、続いて、暗号化処理部1430が、公開暗号化キーKPmediaにより、セッションキーKs1を暗号化処理して、データバスBS3に与える(ステップS614)。

メモ리카ード200からは、暗号化処理部1430からの暗号化セッションキー[Ks] Kmediaを、携帯電話機105を通じて、携帯電話機107のメモ리카ード202に対して送信する(ステップS616)。

5 メモ리카ード202においては、メモリインタフェース1200を介して、データバスBS3に与えられた受信データを、復号処理部1404が、秘密復号キーKmediaにより復号処理することにより、セッションキーKsを復号し抽出する(ステップS618)。さらに、メモ리카ード202では、Ks1発生器1432と同様の構成を有するKs2発生部1432'がセッションキーKs2を生成する(ステップS620)。

10 続いて、メモ리카ード202では、まず、暗号化処理部1406は、データバスBS3を介してメモリ1412中のKPCard(1)保持部1405から与えられる公開暗号化鍵KPCard(1)を受け取り、切換えスイッチ1409が接点Paが閉じる状態となっているので、暗号化処理部1406は、接点Paを介してKs2発生部1432'から与えられるセッションキーKs2を受け取る。
15 暗号化処理部1406は、切換えスイッチ1435が接点Peが閉じる状態が選択されているので、復号処理部1404からのセッションキーKs1により、公開暗号化鍵KPCard(1)およびセッションキーKs2を暗号化してデータバスBS3に与える(ステップS622)。

20 携帯電話機107を介して、暗号化処理部1406により暗号化されたデータ[KPCard(1)、Ks2] Ks1がメモ리카ード200に対して送信される(ステップS624)。

25 メモ리카ード200においては、メモ리카ード202から送信された暗号化データを復号処理部1410がセッションキーKs1により復号化して、メモ리카ード202の公開暗号化キーKPCard(2)およびセッションキーKs2を復号抽出する(ステップS626)。このとき、切換えスイッチ1435では接点Pfが閉じており、Ks1発生回路1432からのセッションキーKs1が復号処理部1410に与えられている。

続いて、メモ리카ード200では、メモリ1412中のレジスタ1500から、ライセンスキーKc、ライセンスIDデータLicense-ID、ユーザID

データ User-ID とが読み出される (ステップ S629)。

さらに、メモリカード 200 の暗号化処理部 1414 は、復号処理部 1410
において抽出されたメモリカード 202 における公開暗号化キー Kp card
(2) により、ライセンスキー Kc、ライセンス ID データ License-ID
5 ID、ユーザ ID データ User-ID とを暗号化する (ステップ S634)。

メモリカード 200 の暗号化処理部 1414 により暗号化されたデータは、切
換えスイッチ 1409 (接点 Pd が閉じている) を介して、さらに、暗号化処理
部 1406 に与えられ、暗号化処理部 1406 は、データ [Kc, License
e-ID, User-ID] Kcard (2) をメモリカード 202 のセッション
10 キー Ks2 により暗号化する (ステップ S636)。このとき、切換えスイ
ッチ 1435 は、接点 Pg が閉じており、復号処理回路 1410 からのセッション
キー Ks2 が暗号化処理部 1406 に与えられている。

続いて、メモリカード 200 は、携帯電話機 105 を介して、メモリカード 2
02 に対して、暗号化されたデータ [[Kc, License-ID, User
15 -ID] Kcard (2)] Ks2 を送信する (ステップ S638)。

メモリカード 202 においては、メモリカード 200 から送信されたデータを
復号処理部 1410 により、セッションキー Ks2 に基づいて復号化処理する
(ステップ S641)。さらに、メモリカード 202 は、秘密復号キー Kcar
d (2) に基づいて、データ [Kc, License-ID, User-ID]
20 Kcard (2) を復号し、復号されたライセンスキー Kc、ライセンス ID デ
ータ License-ID、ユーザ ID データ User-ID をメモリ 1412 中
のレジスタ 1500 に格納する (ステップ S643)。

一方、メモリカード 200 は、レジスタ 1500 よりライセンスキー Kc、ラ
イセンス ID データ License-ID、ユーザ ID データ User-ID を消
25 去し (ステップ S644)、暗号化コンテンツデータ [Dc] Kc をメモリ 14
12 から読み出し、メモリカード 202 に対して送信する (ステップ S646)。

メモリカード 202 は、受信した暗号化コンテンツデータをそのままメモリ
1412 に格納する (ステップ S648)。

すなわち、以上のような構成でも、実施例 8 と同様の動作を実現できる。

なお、以上説明してきた各実施例において、配信データとしてコンテンツデータに付随する非暗号化データ、たとえば、上記音楽データの曲名、実演者（歌手、演奏家等）、作曲家、作詞家等の当該音楽データ（コンテンツデータ）に関する著作権データや音楽サーバ30に対するアクセス情報等を、付加情報D_iとして暗号化コンテンツデータ併せて配信することも可能である。この付加データD_iは、配信、移動、複製においてはコンテンツデータとともに処理され、再生時には分離されてコンテンツデータとは個別にアクセス可能となるように、暗号化コンテンツデータと同じメモリ1412に記録される。

この発明を詳細に説明し示してきたが、これは例示のためのみであって、限定となつてはならず、発明の精神と範囲は添付の請求の範囲によってのみ限定されることが明らかに理解されるであろう。

請求の範囲

1. 暗号化コンテンツデータを受けて記録するためのメモリカードであって、

前記メモリカードに対応して予め定められた第1の公開暗号化鍵によって暗号
5 化されたデータを復号化するための第1の秘密復号鍵を保持する第1の鍵保持部
(1402)と、

前記暗号化コンテンツデータの通信ごとに更新されて配信され、前記第1の公
開暗号化鍵によって暗号化された第1の共通鍵を受けて、復号処理するための第
1の復号処理部(1404)と、

10 前記メモリカードごとに異なる第2の公開暗号化鍵を保持するための第2の鍵
保持部(1405)と、

前記第2の公開暗号化鍵を、前記第1の共通鍵に基づいて暗号化し、出力する
ための第1の暗号化処理部(1406)と、

前記第2の公開暗号化鍵で暗号化され、さらに前記第1の共通鍵で暗号化され
15 たコンテンツキーを受け、前記第1の共通鍵に基づいて復号化するための第2の
復号処理部(1410)と、

前記第2の復号処理部の出力を受けて、格納するための第1の記憶部(141
2)と、

前記第2の公開暗号化鍵によって暗号化されたデータを復号化するための第2
20 の秘密復号鍵を保持する第3の鍵保持部(1415)と、

前記第1の記憶部に格納されたデータに基づいて、前記第2の秘密復号鍵によ
り前記コンテンツキーを復号するための第3の復号処理部(1416)とを備え
る、メモリカード。

2. 前記第1の記憶部は、前記コンテンツキーに基づいて復号できる前記暗号化
25 コンテンツデータを受けて格納する、請求項1記載のメモリカード。

3. 前記メモリカードは、

外部から指示される動作モードに応じて、前記メモリカードの動作を制御する
ための制御部(1420)をさらに備え、

前記第1の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータ

の再生動作が指示されるのに応じて、前記第3の復号処理部からの前記コンテンツキーを受けて、前記第1の共通鍵に基づいて暗号化して出力し、

前記第1の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力する、請求項
5 2記載のメモ리카ード。

4. 前記第2の復号処理部は、前記第2の公開暗号化鍵で暗号化され、さらに前記第1の共通鍵で暗号化されて、前記コンテンツキーとともに配信されるライセンス情報データを受け、前記第1の共通鍵に基づいて復号し、

前記第3の復号処理部は、前記第2の復号処理部から与えられる、第1の共通
10 鍵について復号され前記第2の公開暗号化鍵については暗号化された状態の前記ライセンス情報データを復号し、

前記第3の復号処理部からの復号された前記ライセンス情報データを格納するための第2の記憶部（1500）をさらに備える、請求項3記載のメモ리카ード。

5. 前記メモ리카ードは、

15 前記メモ리카ードに対応して予め定められた第1の公開暗号化鍵を保持し、外部に出力可能な第4の鍵保持部（1440）をさらに備える、請求項1記載のメモ리카ード。

6 前記第1の記憶部は、前記コンテンツキーに基づいて復号できる前記暗号化コンテンツデータを受けて格納する、請求項5記載のメモ리카ード。

20 7. 前記メモ리카ードは、

外部から指示される動作モードに応じて、前記メモ리카ードの動作を制御するための制御部をさらに備え、

前記第1の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記第3の復号処理部からの前記コンテンツ
25 ツキーを受けて、前記第1の共通鍵に基づいて暗号化して出力し、

前記第1の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力する、請求項
6記載のメモ리카ード。

8. 前記第2の復号処理部は、前記第2の公開暗号化鍵で暗号化され、さらに前

記第1の共通鍵で暗号化されて、前記コンテンツキーとともに配信されるライセンス情報データを受け、前記第1の共通鍵に基づいて復号し、

前記第3の復号処理部は、前記第2の復号処理部から与えられる、第1の共通鍵について復号され前記第2の公開暗号化鍵については暗号化された状態の前記
5 ライセンス情報データを復号し、

前記第3の復号処理部からの復号された前記ライセンス情報データを格納するための第2の記憶部をさらに備える、請求項7記載のメモリカード。

9. 前記メモリカードは、

第2の共通鍵を生成するキーデータ生成部と、

10 前記第2の共通鍵を、前記第1の公開暗号化鍵によって暗号化するための第2の暗号化処理部とをさらに備え

暗号化された前記第2の共通鍵は、前記メモリカードから前記他のメモリカードに送信される、請求項1記載のメモリカード。

10. 前記メモリカードは、

15 少なくとも前記第1の暗号化処理部と、前記第1の復号処理部と、前記第2の復号処理部と、前記第3の復号処理部とが設けられ、第三者には読出可能なセキュリティ領域（TRM）と、

前記第1の記憶部が設けられ、第三者に読出可能なデータ領域とを備える、請求項2または6記載のメモリカード。

20 11. 前記メモリカードは、

少なくとも前記第1の暗号化処理部と、前記第1の復号処理部と、前記第2の復号処理部と、前記第3の復号処理部と、前記第2の記憶部とが設けられ、第三者には読出可能なセキュリティ領域と、

25 前記第1の記憶部が設けられ、第三者に読出可能なデータ領域とを備える、請求項4または8記載のメモリカード。

12. 前記第1の記憶部は、前記暗号化コンテンツデータに付随した非暗号化データを、前記暗号化コンテンツデータとともに受けて格納する請求項2または6記載のメモリカード。

13. 暗号化データと前記暗号化データを復号するための復号情報データを受け

て記録するためのメモ리카ードであって、

前記暗号化データを格納する第1の記憶部(1412)と、

前記メモ리카ードに対応して予め定められた第1の公開暗号化鍵と自身の認証
データとを公開認証鍵により復号できるように暗号化して保持し、外部に対して
5 出力可能な第1の鍵保持部(1442)と、

第1の公開暗号化鍵によって暗号化されたデータを復号化するための第1の秘
密復号鍵を保持する第2の鍵保持部(1402)と、

前記復号情報データの通信ごとに更新されて送信され、前記第1の公開暗号化
鍵によって暗号化された前記第1の共通鍵を受けて、復号処理するための第1の
10 復号処理部(1404)と、

前記メモ리카ードごとに異なる第2の公開暗号化鍵を保持するための第3の鍵
保持部(1405)と、

前記復号情報データの通信ごとに更新される第2の共通鍵を生成するセッシ
ョンキー発生部(1432)と、

15 前記第2の公開暗号化鍵と前記第2の共通鍵を、前記第1の共通鍵に基づいて
暗号化し、出力するための第1の暗号化処理部(1406)と、

外部にて前記第2の公開暗号化鍵によって暗号化され、さらに第2の共通鍵によ
って暗号化された前記復号情報データを前記第2の共通鍵に基づいて復号するた
めの第2の復号処理部(1410)と、

20 前記第2の復号処理部の出力である前記第2の公開暗号化鍵によって暗号化され
た前記復号情報データを格納する第2の記憶部(1500)と、

前記第2の公開暗号化鍵によって暗号化されたデータを復号するための第2の
秘密復号鍵を保持する第4の鍵保持部(1415)と、

前記第2の記憶部に格納されたデータを前記第2の秘密復号鍵に基づいて復号
25 し、前記復号情報データを抽出するための第3の復号処理部(1416)とを備
える、メモ리카ード。

14. 前記メモ리카ードは、

前記公開認証鍵を保持する第4の鍵保持部(1450)と、

前記公開認証鍵によって復号できるように暗号化された外部から与えられる自

身以外の第3の公開暗号化鍵と、自身以外の第2の認証データを復号して抽出する第4の復号処理部(1452)と、

前記第4の復号処理部により抽出された前記第2の認証データに基づいて認証処理を行ない、認証できない場合、前記復号情報データの出力を禁止する制御部(1420)と、

前記セッションキー生成部にて通信ごとに更新した第2の共通鍵を、前記第3の公開暗号化鍵に基づいて暗号化して出力する第3の暗号化処理部(1406)と、

外部からの自身以外の固有の第4の公開暗号化鍵に基づいて暗号化を行なうための第3の暗号処理部(1414)をさらに備え、

外部からの復号情報データの出力要求があり、かつ、前記制御部が復号情報データの出力を禁止しない場合、

- i) 前記第2の復号処理部は、第2の共通鍵によって暗号化された前記第1の共通鍵、または第4の公開暗号化鍵および第1の共通鍵をさらに復号出力し、
- 15 ii) 前記第2の復号処理部にて前記第4の公開暗号化鍵が抽出された場合、前記第3の復号手段は、前記第1の記憶部に記録されたデータから復号情報データを抽出し、前記第3の暗号化処理部は、前記第3の復号処理部の出力を前記第2の復号処理部にて出力された第4の公開暗号化鍵にて暗号化して、さらに、第1の暗号化処理部は、第3の暗号化処理部の出力を前記第2の復号処理部にて抽出された第2の共通鍵に基づいて暗号化して出力し、

- 20 iii) 前記第2の復号処理部にて前記第2の共通鍵のみが抽出された場合、前記第2の復号処理手段は、前記第1の記憶部に格納されたデータから復号情報データを抽出し、前記第3の暗号化処理部は、前記第2の復号処理部の出力を、前記第2の復号処理部にて抽出された第2の共通鍵に基づいて暗号化出力する、
- 25 請求項13記載のメモリカード。

15. 前記復号情報データは、前記復号情報データのメモリカードからの出力を制御するためのアクセス制御データをさらに含み、

前記第3の復号部にて前記第2の公開暗号化鍵によって暗号化された復号再生情報から抽出した前記アクセス制御情報を格納する第3の記憶部をさらに備え、

前記制御部は、前記第 3 の記憶部に格納された前記アクセス制御データに基づいて復号情報データの出力を禁止する、請求項 1 4 記載のメモリカード。

1 6。前記メモリカードの記録空間は、

第三者に読出不能かつ書替不可能なセキュリティ領域と、

- 5 第三者に読出可能であり、格納データはメモリカード固有の暗号化が施されている準セキュリティ領域と、

第三者に読出および書替可能な非セキュリティ領域とに区分され、

前記セキュリティ領域は、前記第 1、第 3 の鍵保持部および第 3 の記憶部を含み、

- 10 前記準セキュリティ領域は、前記第 2 の記憶部を含み、

前記非セキュリティ領域は、第 1 の記憶部を含む、請求項 1 5 記載のメモリカード。

1 7。前記準セキュリティ領域および前記非セキュリティ領域は、同一メモリ上に配置される請求項 1 6 記載のメモリカード。

- 15 1 8。暗号化データと前記暗号化データを復号するための復号情報データを受けて記録するためのメモリカードであって、

ERROR: stackunderflow
OFFENDING COMMAND: ~
STACK: